



***Cabinet for Health and Family Services (CHFS)  
Information Technology (IT) Policy***



**065.015 Application Audit and Accountability**

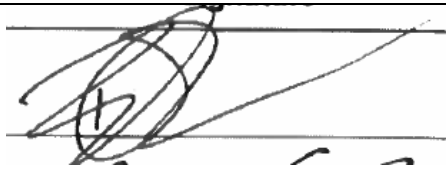
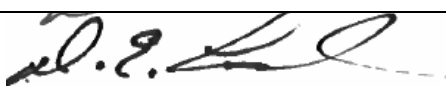
**Version 2.2  
February 19, 2018**

065.015 Application Audit and Accountability	Current Version: 2.2
065.000 Application Development	Review Date: 02/19/2018

## Revision History

Date	Version	Description	Author
2/23/2011	1.0	Effective Date	CHFS IT Policies Team Charter
2/19/2018	2.2	Revision Date	CHFS OATS Policy Charter Team
2/19/2018	2.2	Review Date	CHFS OATS Policy Charter Team

## Sign-Off

Sign-off Level	Date	Name	Signature
IT Executive, Office of the Secretary (or designee)	2/19/2018	Bernard "Deck" Decker	
CHFS Chief Information Security Officer (or designee)	2/19/2018	DENNIS E. LEBEK	

065.015 Application Audit and Accountability	Current Version: 2.2
065.000 Application Development	Review Date: 02/19/2018

## Table of Contents

<b>065.015 APPLICATION AUDIT AND ACCOUNTABILITY .....</b>	<b>5</b>
<b>1 POLICY OVERVIEW.....</b>	<b>5</b>
1.1 PURPOSE .....	5
1.2 SCOPE .....	5
1.3 MANAGEMENT COMMITMENT.....	5
1.4 COORDINATION AMONG ORGANIZATIONAL ENTITIES .....	5
1.5 COMPLIANCE .....	5
<b>2 ROLES AND RESPONSIBILITIES .....</b>	<b>6</b>
2.1 CHIEF INFORMATION SECURITY OFFICER (CISO) .....	6
2.2 SECURITY/PRIVACY LEAD .....	6
2.3 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY OFFICER .....	6
2.4 CHFS STAFF AND CONTRACT EMPLOYEES .....	6
2.5 SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....	7
<b>3 POLICY REQUIREMENTS .....</b>	<b>7</b>
3.1 AUDITABLE EVENTS .....	7
3.2 CONTENT OF AUDITABLE EVENTS .....	7
3.3 AUDIT STORAGE CAPACITY .....	7
3.4 RESPONSE TO AUDIT PROCESSING FAILURES .....	7
3.5 AUDIT REVIEW, ANALYSIS, AND REPORTING.....	7
3.6 AUDIT REDUCTION AND REPORT GENERATION.....	7
3.7 TIME STAMPS.....	8
3.8 PROTECTION OF AUDIT INFORMATION .....	8
3.9 AUDIT RECORD RETENTION .....	8
3.10 AUDIT GENERATION .....	8
<b>4 POLICY MAINTENANCE RESPONSIBILITY .....</b>	<b>8</b>
<b>5 POLICY EXCEPTIONS .....</b>	<b>8</b>
<b>6 POLICY REVIEW CYCLE.....</b>	<b>8</b>
<b>7 POLICY REFERENCES .....</b>	<b>8</b>

065.015 Application Audit and Accountability	Current Version: 2.2
065.000 Application Development	Review Date: 02/19/2018

## Policy Definitions

- **Auditable Events:** events defined by federal, state, and agency guidelines, needing to be audited and retained by the agency for the defined period of time. Auditable events can include but are not limited to: number of failed system log-on attempts, password changes, system errors, printing, changes, updates, deletion may to the system, and application errors.
- **Audit Log Failure:** events defined by federal and state guidelines in which logs being captured show issues or errors. Audit log failures can include but are not limited to: software/hardware errors, failures in the audit capturing mechanisms, audit storage capacity being reached or exceeded, location of access, and severity of captured information.
- **Confidential Data:** Defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Coordinated Universal Time:** is the time standard commonly used across the world, basis for civil time today. This 24-hour time standard is kept using highly precise atomic clocks combined with Earth's rotation.
- **Greenwich Mean Time:** is the clock time at the Royal Observatory in Greenwich, London. GMT is the same all year round and is not affected by Summer Time or Daylight Saving Time.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)

065.015 Application Audit and Accountability	Current Version: 2.2
065.000 Application Development	Review Date: 02/19/2018

# 065.015 Application Audit and Accountability

Category: 065.000 Application Development

## 1 Policy Overview

### 1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through an audit and accountability policy. This document establishes the agency's Application Audit and Accountability Policy which helps manage risks and provides guidelines for security best practices regarding audit record retention

### 1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

### 1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and Office of the Secretary IT Executive. Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restricted access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

### 1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted with OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking an exception to this policy.

### 1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

065.015 Application Audit and Accountability	Current Version: 2.2
065.000 Application Development	Review Date: 02/19/2018

## **2 Roles and Responsibilities**

### ***2.1 Chief Information Security Officer (CISO)***

This position is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This designated position is responsible to adhere to this policy.

### ***2.2 Security/Privacy Lead***

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role along with the CHFS OATS Information Security (IS) Team is responsible for the adherence of this policy.

### ***2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer***

An attorney within CHFS Office of Legal Services (OLS) fills the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position. This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or CHFS OATS Information Security (IS) Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position is responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notifications in accordance with HIPAA rules and regulations.

### ***2.4 CHFS Staff and Contract Employees***

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

065.015 Application Audit and Accountability	Current Version: 2.2
065.000 Application Development	Review Date: 02/19/2018

## **2.5 System Data Owner and System Data Administrators**

It is the responsibility of these management/lead positions, to work with the application's development team to document components that are not included in the base server build and ensure backup are conducted in line with business needs. This individual(s) will be responsible to work with Enterprise, agency, and application technical and business staff to provide full recovery of all the application functionality and meet federal and state regulations for disaster recovery situations.

# **3 Policy Requirements**

## **3.1 Auditable Events**

The agency will ensure that the information system or components are capable of auditing events defined by federal and state regulations. The agency will coordinate security functions and controls with other organizational entities to ensure required auditable events or related data are being captured. CHFS shall follow the CHFS Audit and Accountability Procedure for additional information on audit logs, events, and more.

## **3.2 Content of Auditable Events**

The information system will generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

## **3.3 Audit Storage Capacity**

The agency will allocate audit storage capacity in accordance with all federal and state regulations and guidance.

## **3.4 Response to Audit Processing Failures**

The information system and/or its components will alert designated agency personnel in the event of an audit log failure where agency action will then be taken.

## **3.5 Audit Review, Analysis, and Reporting**

The CHFS IS Team will work with System Data Owners, or designee(s) whom receive audits, reports, and analysis, as directed by federal and state regulations, will regularly review and analyze the information system audit records and report issues or findings to management.

## **3.6 Audit Reduction and Report Generation**

The information system provides an audit reduction report generation capability that supports functions for on demand audit review, analysis and reporting requirements, and after the fact investigation of security incidents. The information system will not alter the original content or time ordering of any audit records.

065.015 Application Audit and Accountability	Current Version: 2.2
065.000 Application Development	Review Date: 02/19/2018

### **3.7 Time Stamps**

The information system will use internal system clocks that can be mapped to Coordinated Universal Time (UTC), Greenwich Mean Time (GMT) to generate time stamps. The agency will meet federal and state defined granularity of time measurements on audit logs.

### **3.8 Protection of Audit Information**

The information system will protect audit information and audit tools from unauthorized access, modifications, and deletion capabilities. The agency will have compensating controls in place to prevent any unauthorized action to be taken on audit information.

### **3.9 Audit Record Retention**

The agency will retain audit records to provide support for after the fact investigations of security incidents and to meet all state and federal regulatory retention requirements. Agencies will follow CHFS 040.101 Application Backup Policy.

### **3.10 Audit Generation**

The information system will provide audit record generation capability for the auditable events and allow designated agency personnel to select which audible events are to be audited by specific components of the information system.

## **4 Policy Maintenance Responsibility**

The OATS IS Team is responsible for the maintenance of this policy.

## **5 Policy Exceptions**

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

## **6 Policy Review Cycle**

This policy is reviewed at least once annually, and revised on an as needed basis.

## **7 Policy References**

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 040.101 Application Backup Policy
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS OATS Procedure: CHFS Audit and Accountability Procedure

065.015 Application Audit and Accountability	Current Version: 2.2
065.000 Application Development	Review Date: 02/19/2018

- Internal Revenue Services (IRS) Publication 1075
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information